16 STRON EKSTRA

RAPORTUJĄCY

BEZPIECZNA BANKOWOŚĆ ELEKTRONICZNA

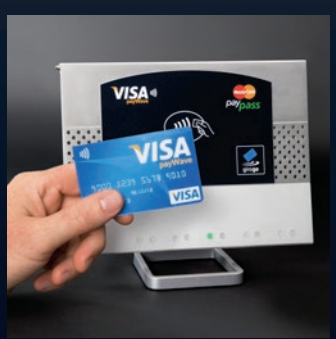
Komputer Świat

BEZPIECZNA BANKOWOŚĆ ELEKTRONICZNA

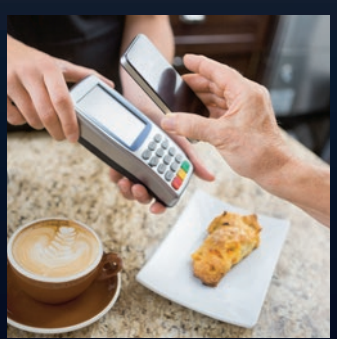
- Zobacz, jak rozwija się **bankowość elektroniczna**
- Odkryj **nowoczesne metody płacenia**
- Poznaj **tajniki bezpiecznej bankowości online**

TO MUSISZ WIEDZIEĆ!

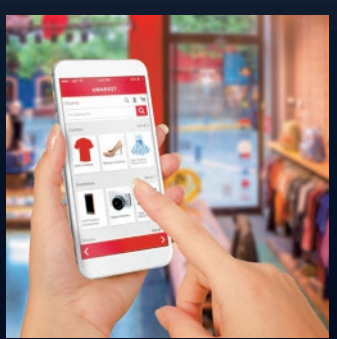
- **Jak zacząć** korzystać z usług banku online



- Na co polują **hakerzy** i jakie są ich metody



- **BLIK** – wyjątkowy sposób płacenia i wypłacania



- Najważniejsze pojęcia dotyczące **banków w sieci**

RAPORT
bankowość elektroniczna

JAK ZMIENIA SIĘ

Szybkie przelewy bez wychodzenia z domu, dostęp do kont walutowych i płatności na telefon. Tak wygląda dzisiejsza bankowość. *Jednak nie zawsze tak było. Pierwszy bank utworzono w 1156 roku w Wenecji. Było to miejsce, do którego dostęp mieli tylko najbogatsi. Zobaczmy, jak zmieniała się bankowość na przestrzeni wieków i ostatnich lat. Jak będzie wyglądała w przyszłości?*

Zdaniem badaczy, pierwszy bank utworzono w 1156 roku w Wenecji. To data, którą można uznać za oficjalny debiut bankowości. Instytucje te znajdowały się początkowo w rękach najbogatszych włoskich rodzin. Ówczesny bank był miejscem, w którym swój kapitał i oszczędności lokowali najzamożniejsi obywatele, w tym kupcy i głowy państw. To były elitarne instytucje dla wybranych. Do zadań późniejszych banków emisyjnych należało również bicie monet. Jednak kiedy bankierzy i władcy zaczęli emitować pieniądze, które nie miały odzwierciedlenia w kruszcu, sytuacja zaczęła się zmieniać. Takie „psucie pieniądza" budziło oburzenie społeczne i było niekorzystne dla gospodarki.

Istotne zmiany nastąpiły dopiero w 1668 roku, kiedy to szwedzki parlament utworzył Szwedzki Bank Państwowy. Był to pierwszy bank centralny w Europie, który odpowiadał za funkcjonowanie systemu finansowego oraz prowadzenie bieżącej polityki pieniężnej państwa. To była też instytucja, która jako pierwsza wydawała kwity papierowe, które można było zbywać innym. Tymi śladami szybko podążyły inne kraje Europy.

Początki bankowości komercyjnej

Liczba banków centralnych zwiększała się z każdym rokiem. Na początku XIX wieku było ich 20, w latach trzydziestych XX wieku było ich już około 30, a w latach sześćdziesiątych było ich ponad 160. Bankowość bardzo szybko się rozwijała wraz z uprawnieniami tych instytucji, które nie tylko odpowiadały za politykę pieniężną państwa i emisję pieniędzy, ale również zajmowały się kredytowaniem. Trzeba dodać, że funkcja banku centralnego była nadawana danej instytucji na pewien okres, zazwyczaj na 20 lat. Kiedy dobiegał końca, najczęściej zmieniano nazwę i ponownie nadawano przywilej. Banki powoli zaczęły zmieniać sposób funkcjonowania. Obok banku centralnego pojawiały się inne instytucje, które nie pełniły tej funkcji, ale które oferowały podobne usługi, bez możliwości emisji pieniądza i kontrolowania polityki pieniężnej państwa. Był to początek ery banków komercyjnych, które funkcjonowały na szerszą skalę, a swoje usługi oferowały niemal każdemu.

Jak działają banki?

Do banku idziemy zazwyczaj w dwóch celach. Albo mamy nadwyżkę pieniędzy i chcemy ją ulokować z zyskiem, albo nie mamy środków i chcemy wziąć kredyt. Bank zarabia zarówno na inwestorach, jak i kredytobiorcach. Bierze pieniądze od klientów i nimi obraca, najczęściej za symboliczny procent, jednocześnie pożycza je już na zupełnie innych zasadach. Można by stwierdzić, że bank zarabia na obracaniu nie swoimi pieniędzmi. I tak z reguły jest. Czym więcej osób zdecyduje się lokować pieniądze i otwierać konta, tym większymi środkami bank może dysponować. Jak banki zdobywają nowych klientów? Nie bez znaczenia jest funkcjonalność, bezpieczeństwo i wizerunek.

Przed wprowadzeniem powszechnej bankowości elektronicznej banki kojarzyły się nam z marmurowymi pałacami, długimi kolejkami i bankierami w garniturach. Był to wypracowany przez lata wizerunek, który miał ukazywać nam bank jako poważną instytucję, której można bezpiecznie powierzyć wszystkie oszczędności. Jeśli klienci tracą zaufanie do banku, rezygnują z jego usług, a bank ma wówczas mniejsze kwoty na swoje inwestycje i kredyty, które stanowią główne źródło jego dochodów.

Nowoczesne banki działają inaczej i rezygnują z opłat

Postęp technologiczny zmienia między innymi nasze oczekiwania wobec banków. Wiemy już, że bank musi zdobywać klientów, aby zarabiać. Dziś nie wystarczą jednak marmury i bankierzy w garniturach, którzy z uśmiechem przyjmują nasze pieniądze. Komercjalizacja banków i szeroki dostęp do nowoczesnych technologii sprawiły, że oczekujemy od instytucji bankowych wygodnej obsługi. Banki muszą nadążyć za postępem i dlatego stale oferują nowe funkcje, systemy i produkty.

Zmieniają się też sposoby zarabiania banków, a tym samym również ich funkcjonowanie. Najlepszym przykładem jest tutaj rezygnacja z płatnych rachunków i odpłatnego wydawania kart płatniczych. Jeszcze kilka lat temu banki pobierały miesięczne opłaty za utrzymanie rachunków i korzystanie z kart oraz bankomatów. Dzisiaj wszystko jest darmowe. Dlaczego? Bo właśnie tego oczekujemy jako klienci. Banki kuszą nas darmowymi kontami, abyśmy tylko wpłacali swoje oszczędności. Dysponowanie nimi przynosi bankowi o wiele większe zyski niż miesięczna opłata za prowadzenie rachunku.

BANKOWOŚĆ?

Dzisiejsze banki to już nie eleganckie marmury

Sektor bankowy to jedna z najszybciej rozwijających się branż. Aby zdobywać nowych klientów, stale trzeba wprowadzać nowoczesne technologie, które nie tylko zwiększają funkcjonalność, ale i bezpieczeństwo. Pokochaliśmy nowe technologie i lubimy mieć stały dostęp do kont i możliwość płacenia w dowolnym miejscu, nawet przy użyciu telefonu czy opaski elektronicznej. Banki doskonale o tym wiedzą, dlatego tak chętnie oferują nam coraz to nowe funkcje. Instytucje, które stoją w miejscu i nie odpowiadają na potrzeby klientów, po prostu upadają lub zostają przejęte przez innych.

Dziś mamy niemal nieograniczone możliwości, które dają nam nowe technologie. Robimy zakupy online, płacimy za nie jednym kliknięciem, a to wszystko wygodnie bez wychodzenia z domu. Wizerunek marmurowego pałacu z kilometrowymi kolejkami do okienka nie pasuje do naszych czasów. Banki nie tylko zmieniły wizerunek i promują się na przytulne niczym kawiarnie zakątki, ale także sposób funkcjonowania.

Rozwój bankowości internetowej wcale nie oznacza jednak końca stacjonarnych placówek. Z pewnością nie nastąpi to zbyt szybko. O ile lubimy samodzielnie wykonywać proste czynności, takie jak sprawdzanie historii płatności lub przelewy przez internet, tak bardziej skomplikowane operacje, na przykład branie kredytu hipotecznego i korzystanie z usług maklerskich, wciąż wolimy wykonywać w obecności pracownika banku – specjalisty. W grę wchodzą przecież nasze pieniądze, często oszczędności życia.

Banki oferują nam dziś bardzo wiele, jeśli chodzi o elektroniczną bankowość i obsługę bezgotówkową. Jeżeli tylko pojawi się jakaś technologiczna ciekawostka, zaraz mamy ją w ofercie któregoś z banków. Tak było między innymi z płatnościami BLIK.

Zalet płatności zdalnych jest wiele. Poza szybkością przekazywania środków i możliwością dokonywania zakupów online, jedną z najważniejszych w naszym kraju jest możliwość zwrotu towaru bez podania przyczyny w ciągu 14 dni od dokonania zakupu. W tradycyjnym handlu takiej możliwości nie mamy: zakupiony towar, o ile jest pełnowartościowy, zwrócimy tylko wtedy, gdy sprzedawca daje taką możliwość, co należy do rzadkości. Przedmiot kupiony przez internet możemy oddać i sprzedający musi nam zwrócić pieniądze (choć są tutaj wyjątki, jak na przykład produkty szybko psujące się, treści cyfrowe czy towary nabyte od osób prywatnych).

JAK WYGLĄDA PRZYSZŁOŚĆ BANKOWOŚCI?

Zmiany dzieją się na naszych oczach. Pamiętamy jeszcze długie kolejki do okienek w celu prostego sprawdzenia stanu konta, później pojawiły się bankomaty, a dziś możemy każdą czynność wykonać z domu. Wystarczy smartfon i internet. Analitycy szacują, że ten trend się utrzyma. Banki wciąż będą musiały nadążyć za potrzebami nowoczesnego konsumenta, a ten jest mobilny i ma duże oczekiwania. Klient nie chce być ograniczany w jakikolwiek sposób, chce realizować transakcje na portalach społecznościowych i za pomocą telefonu. Szybko, wygodnie i bezpiecznie.

To nie jest wizja rodem z filmu SF. To nasza codzienność. Stale rezygnujemy z gotówki na rzecz wirtualnych kart i środków płatniczych. Korzystamy z Android Pay, BLIK-a i Apple Pay. Do tego banki stale zwiększają swoje zabezpieczenia i ułatwiają nam wszelkie formalności. Dziś już nie musimy nawet wychodzić z domu, aby założyć konto bankowe. A co przyniesie jutro?

Można sobie to jedynie wyobrażać. Wielu z nas życzyłoby sobie łatwiejszej komunikacji z bankami. Już mamy dostęp do wirtualnych oddziałów, w których porozmawiamy albo z botem, albo z żywym konsultantem przez wideoczat. Czy to prawie szczyt naszych osiągnięć technologicznych?

Dalsze zmiany z pewnością będą szły w kierunku rozwoju sztucznej inteligencji oraz zwiększania poziomu bezpieczeństwa – w tym segmencie zawsze będzie coś do zrobienia. Dodatkowo banki coraz chętniej patrzą w stronę technologii blockchain.

Fot. Brian Jackson, Alexander Kirch, Ariadna De Raadt/123rf.com

RAPORT
bankowość elektroniczna

NOWOCZESNA BANKOWOŚĆ ELE

NAUCZ SIĘ Z NIEJ KORZYSTAĆ W KILKU KROKACH

Banki coraz bardziej idą nam na rękę**, dzięki czemu założenie konta z dostępem przez elektroniczne kanały jest dziś bardzo łatwe. Gdy już będziemy mieć takie konto, praktycznie **wszystko w banku załatwimy bez wychodzenia z domu!

Bankowość elektroniczna daje wiele możliwości, w tym obsługę rachunków bankowych bez konieczności wychodzenia z domu. Obsługa rachunku bankowego odbywa się przy użyciu publicznej sieci telefonicznej lub internetowej. Jeszcze do niedawna każda operacja – założenie konta, zrobienie prostego przelewu czy sprawdzenie salda – wymagała od nas wizyty w placówce banku, poczty lub skorzystania z bankomatu. To już przeszłość. Zobacz, do czego przydaje się bankowość elektroniczna i jak zacząć z niej korzystać.

Pierwsze kroki

Załóż konto w banku przez internet i zacznij korzystać z bankowości elektronicznej

Korzystanie z bankowości elektronicznej jest wygodne, bezpieczne (w przypadku stosowania się do pewnych zasad, które omówimy w następnych artykułach), a przede wszystkim powszechne. Jak zacząć?

Dzisiaj zdecydowana większość banków daje swoim klientom dostęp do bankowości elektronicznej. Nawet jeśli założyłeś konto wiele lat temu, jest spora szansa, że twój bank również oferuje dostęp do rachunków przez internet. Wystarczy, że zadzwonisz na infolinię i spytasz o dane do logowania. Żeby mieć dostęp do bankowości elektronicznej, złóż odpowiednią dyspozycję (zrobisz to telefonicznie, wysyłając wiadomość e-mail lub odwiedzając placówkę banku). Otrzymasz wtedy zestaw narzędzi, które umożliwią ci logowanie na stronę banku. Żeby wejść na swoje konto, potrzebny będzie numer klienta, hasło, a do przeprowadzania niektórych operacji kod z listy haseł jednorazowych czy kod wysłany przez bank SMS-em w momencie realizowania transakcji.

Nie masz jeszcze konta w banku? Założysz je w kilka chwil, wypełniając formularz rejestracyjny na stronie internetowej. Po wysłaniu wniosku zostaniesz poproszony o potwierdzenie swojej tożsamości. Metod jest kilka. W zależności od banku będziesz mógł:

- wysłać skan swojego dowodu osobistego;
- podpisać umowę z bankiem, którą przywiezie do ciebie przedstawiciel;
- wysłać wiadomość SMS z kodem aktywacyjnym;
- wykonać przelew z innego banku na symboliczną kwotę (najczęściej jest to 1 zł, który i tak zostaje zwrócony).

Cała procedura założenia rachunku trwa nie więcej niż 5 minut, a potem otwiera się dla ciebie cały świat bankowości elektronicznej, który upraszcza wiele codziennych czynności.

Dlaczego powinieneś korzystać z bankowości elektronicznej

Przyczyna niezwykle szybkiego wzrostu popularności bankowości elektronicznej w naszym kraju wydaje się prosta – przez internet mamy dostęp obecnie do niemal każdej usługi bankowej. Zwłaszcza młode osoby nie wyobrażają już sobie konieczności chodzenia do tradycyjnego oddziału banku na przykład w celu wykonania przelewu. Jak wygląda popularność usług bankowości internetowej wśród młodych Polaków? Odpowiedź na to pytanie znajdziemy w najnowszych badaniach Gemiusa. Z badań przeprowadzonych przez IIBR na 4 tysiącach internautów wynika, że młodzi w wieku 18–24 lat są drugą najliczniejszą grupą odbiorców bankowości elektronicznej w Polsce. Ponad 70 procent z nich korzysta z dostępu do konta online. Najwięcej klientów to natomiast osoby między 25 a 34 rokiem życia (82%). Zdaniem dr. Emila Ślązaka z Katedry Bankowości SGH te wyniki potwierdzają obserwowany za granicą wzrost znaczenia finansowego osób urodzonych w latach osiemdziesiątych XX wieku, które wyróżniają się wysokimi kompetencjami w kontaktach zdalnych (tzw. pokolenie Y).

Dzisiaj nikogo nie trzeba już przekonywać do bankowości elektronicznej. Dzięki niej mamy całodobowy dostęp do naszych pieniędzy. Wystarczy telefon lub komputer z dostępem do internetu i można wykonać dowolną operację – przelew, sprawdzenie historii wypłat, wygenerowanie analizy wydatków czy sprawozdania finansowego, sporządzenie potwierdzenia wpłaty, założenie lokaty czy funduszu inwestycyjnego. Warto zaznaczyć, że każda operacja jest dodatkowo chroniona i wymaga wpisania kodu SMS lub innego potwierdzenia – może to być kod z tokena, dodatkowe hasło zabezpieczające, a nawet odcisk palca lub skan siatkówki oka.

KTRONICZNA

PRAKTYCZNE PRZYKŁADY ZASTOSOWANIA

Wystarczy jedno kliknięcie...

Szybkie przelewy i inne operacje

Wiesz już, jak łatwo zacząć korzystać z bankowości elektronicznej. Zastanawiasz się jeszcze nad korzyściami? Rozpowszechnienie internetu zmieniło życie wszystkich ludzi. Możemy komunikować się z dowolnymi osobami na drugim krańcu świata, mamy szeroki dostęp do multimediów i sklepów. Internet wpłynął również na obrót pieniędzmi i sposoby korzystania z bankowości. Dzisiaj jednym kliknięciem możemy nie tylko dostać się do naszego rachunku bankowego, ale i wykonać wszystkie interesujące nas operacje. Nawet to nie będzie konieczne, jeśli zdefiniujemy w systemie stałe polecenia, na przykład comiesięczne wypłaty. Wyobraź sobie, że do 10 dnia każdego miesiąca musisz uregulować kilkanaście rachunków, w tym na przykład za telefon, internet, gaz, prąd itp. Każdorazowe wpisywanie danych odbiorcy i zlecanie przelewów może być męczące, nawet korzystając z internetu. Można jednak ustawić przelewy cykliczne i określona kwota będzie automatycznie wysyłana do odbiorcy każdego miesiąca.

WYBIERZ NAJLEPSZE KONTO INTERNETOWE

Procedura założenia konta nie różni się zbytnio w poszczególnych bankach. Wszystko sprowadza się do wypełnienia formularza. Jednak zanim to zrobisz, musisz jeszcze wybrać odpowiedni bank. Ten powinien najlepiej odpowiadać twoim potrzebom. Weź pod uwagę takie czynniki, jak częstotliwość:

- wypłat z bankomatów;
- wykonywania przelewów online;
- wizyt w oddziałach;
- korzystania z aplikacji mobilnej czy bankowości internetowej.

Analiza wszystkich tych czynników pomoże dopasować i wybrać najlepszy rachunek. Jeżeli nie masz pewności, jaki produkt będzie dla ciebie najodpowiedniejszy, porównaj tabele opłat i prowizji, które znajdziesz na stronach internetowych banków. Wybierając konto internetowe, zwróć uwagę na czytelność systemu i sposób jego obsługi (wiele banków oferuje możliwość symulowanego przetestowania bankowości internetowej w postaci demo).

Dostęp do zaawansowanych funkcji

Inwestuj z bankowością elektroniczną

Jednym kliknięciem nie tylko dostaniesz się do rachunku. Banki często dają dostęp również do bardziej zaawansowanych funkcji związanych z kredytowaniem, finansowaniem, lokowaniem i inwestowaniem. Niektóre systemy bankowe (na przykład system mBanku, który jest jednym z najbardziej rozbudowanych i nowoczesnych) oferują możliwość zakupu akcji na giełdzie oraz inwestowanie w fundusze.
Korzystając z bankowości elektronicznej, możesz założyć lokatę i bezpiecznie pomnażać oszczędności (najczęściej lokaty są oprocentowane od 1,5 do 3,0 procent w skali roku) lub zacząć inwestować na giełdzie. Wystarczy złożyć odpowiednie polecenie i można kupić akcje jednej z wielu firm lub zainwestować w surowce.

Niższe koszty obsługi, wyższe oprocentowanie lokat

Korzystanie z bankowości elektronicznej to również oszczędność pieniędzy. Zlecenie zwykłego przelewu w oddziale banku kosztuje od 5 złotych w górę, wykonanie przelewu na poczcie to 2,50 złotego. Dodatkowo płatne mogą być różne operacje, na przykład sprawdzenie salda konta w bankomacie. Bankowość elektroniczna daje to wszystko o wiele taniej, a najczęściej po prostu za darmo. Banki odchodzą nawet od opłat za korzystanie z kart debetowych i kredytowych. Jeśli często wykonujesz operacje w oddziałach, bankowość internetowa może być dla ciebie sporą oszczędnością czasu i pieniędzy.
Jest nie tylko taniej, ale i więcej można zarobić na lokatach. Banki oferują inne produkty i warunki dla klientów internetowych i tradycyjnych. Często może zdarzyć się tak, że biorąc kredyt przez internet, zapłacisz niższą ratę niż w przypadku kredytu zaciągniętego w stacjonarnym oddziale banku. Podobnie jest z lokatami. Tutaj również wygrywa bankowość internetowa. Często ta sama lokata może być niżej oprocentowana, jeśli podpiszesz wniosek w stacjonarnym oddziale. Banki chcą w ten sposób odwieść nas od bankowości tradycyjnej. I jest to skuteczne! Coraz więcej banków zamyka swoje drogie w utrzymaniu oddziały na rzecz rozbudowy systemów internetowych.

Śledź stan swojego konta

Gdziekolwiek jesteś i kiedykolwiek chcesz

Bankowość elektroniczna pozwala na bieżąco śledzić stan swoich rachunków bankowych. Wystarczy zalogować się do systemu i możesz zobaczyć historię wpłat i wypłat. Przydaje się to w wielu przypadkach. Zobaczysz na przykład, czy twój szef przelał ci wynagrodzenie, sprawdzisz, ile ostatnio wydałeś za zakupy i ile musisz spłacić kredytu. To wygodne rozwiązanie, które pozwala mieć kontrolę nad finansami z dowolnego miejsca i o każdej porze dnia i nocy.
Doceniają to przede wszystkim przedsiębiorcy, którzy na bieżąco mogą sprawdzać stan swojego firmowego konta i monitorować płatności od swoich kontrahentów. Dodatkowo istnieje możliwość ustawienia powiadomień SMS po każdej wpłacie lub przesyłania dziennych, tygodniowych lub miesięcznych wyciągów z kont na podany adres e-mail.

Weź kredyt lub pożyczkę w dowolnym momencie

Bankowość elektroniczna pozwala również na składanie wniosków, w tym o pożyczkę lub kredyt. Aby to zrobić, wystarczy, że wypełnisz odpowiedni formularz. To ogromna oszczędność czasu, która wyklucza częste wizyty w stacjonarnym oddziale. Zazwyczaj rozpatrzenie podania o kredyt trwa kilka dni, a informację dostajemy listownie, elektronicznie lub telefonicznie.
Mimo rozwoju systemów transakcyjnych oraz coraz większej dostępności usług elektronicznych podpisanie umowy kredytowej na większe kwoty, rzędu kilkuset tysięcy złotych, wciąż wymaga wizyty w oddziale lub osobistego kontaktu z przedstawicielem. Ma to na celu zapewnienie większego bezpieczeństwa i wykluczenie sytuacji, w której cyberprzestępca bierze kredyt na nasze dane.
Dzięki bankowości internetowej klient banku ma łatwy dostęp do własnego rachunku przez całą dobę i z każdego miejsca na świecie – 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. To wygoda i bezpieczeństwo. Dzisiejsze systemy bankowe rozwijają się tak szybko, że każdego miesiąca pojawiają się dodatkowe funkcje i możliwości, takie jak na przykład wymiana walut w systemie czy płatności telefonem bez udziału karty debetowej czy kredytowej. Bankowość elektroniczna to przyszłość i warto być z nią na bieżąco.

Fot. Bloomua, Kantver/123rf.com

RAPORT
bankowość elektroniczna

W TEN SPOSÓB

POZNAJ NAJNOWSZE MOŻLIWOŚCI W ZAKRESIE NOWOCZESNYCH

Odcisk palca czy skan siatkówki naszego oka *wystarczą, żeby szybko autoryzować dowolną płatność, czy to w internecie czy w stacjonarnym sklepie. Jakie jeszcze nowoczesne rozwiązania oferują współczesne banki?*

Karta płatnicza, przelewy za pośrednictwem kart płatniczych czy portfele wirtualne? Znamy to już niemal wszyscy. To dziś popularne metody w świecie, w którym nie ma już miejsca dla gotówki. Czy bankowość internetowa może rozwinąć się jeszcze bardziej? Oczywiście! To się dzieje na naszych oczach. Poznaj najnowocześniejsze metody płatności, z których prawdopodobnie jeszcze nie korzystałeś.

Płatności NFC i HCE

Skoro smartfonem robimy zdjęcia, kręcimy film, przeglądamy na nim strony internetowe, a nawet robimy zakupy online, to dlaczego by nie płacić nim w sklepach stacjonarnych?
Płatności dotykowe telefonem NFC i HCE stają się coraz popularniejsze. Potrzebujesz do tego jedynie urządzenia, które obsługuje jedną z tych technologii, oraz kartę wirtualną z banku, która w przypadku NFC zostanie przypisana do twojej karty SIM w urządzeniu. Po aktywacji usługi u operatora możesz płacić za zakupy w sklepie, zbliżając do terminalu swój telefon zamiast karty kredytowej lub debetowej.
Technologia HCE różni się od NFC tym, że operacje oparte są na chmurze i do ich przeprowadzania nie potrzeba karty SIM. Nie trzeba tym samym podpisywać umowy z operatorem sieci komórkowej. Obecnie użytkownicy kart MasterCard mogą korzystać z tej technologii, jeśli są klientami banku Pekao SA, Getin Bank oraz Santander.

Płatności przez SMS

W zasadzie to nie jest nic nowego i zapewne z tej formy płatności mogłeś już korzystać. Jeśli nie wiesz, o co chodzi, już tłumaczymy – wysyłając SMS na dany numer, zyskujesz dostęp do pewnych usług, które oferują niektóre portale. W ten sposób często też wspomożesz różne akcje charytatywne i weźmiesz udział w wielu konkursach.
Jak to działa w praktyce? Wysyłasz wiadomość i z twojego konta zostanie pobrana określona kwota (jeśli posiadasz telefon na kartę) lub będzie dopisana do rachunku za abonament telekomunikacyjny. Zaletą tego rozwiązania jest to, że płatność odbywa się w ciągu kilka chwil. Minusem jest to, że operator sieci komórkowej pobiera wysoką prowizję.

Płatności tokenem

Wiesz już, że swoim telefonem zapłacisz bez problemu niemal w każdym sklepie. Jednak nie tylko on ma takie funkcje. Bankowość elektroniczna idzie do przodu, a banki, wiedząc o tym, często dają klientom coraz to nowsze i łatwiejsze sposoby na wydawanie pieniędzy. Były płatności w telefonie. Teraz popularne są płatności tokenami, które często przyjmują formę naklejek. Możesz ją przykleić dosłownie wszędzie – nawet do breloczka od kluczy czy pod pierścionkiem. Jak to działa? Czy tokenizacja jest bezpieczna?
Trzeba wspomnieć, że tokenizacja to inaczej ciąg cyfr, który zastępuje numer karty. Technologia ta polega na zakodowaniu danych karty płatniczej w innym urządzeniu. Może to być wspomniana wcześniej specjalna naklejka, a może to być też zegarek czy opaska fitness. Ten rodzaj płatności oferuje między innymi usługa MasterCard Digital Enablement Service (MDES).
Tokenizacja jest w pełni bezpieczna, ponieważ transakcje są chronione podobnie jak w przypadku standardowych płatności kartą. Nawet kiedy złodziej będzie chciał użyć skradzionej opaski z tokenem, i tak będzie musiał podać PIN.

Masterpass i Visa Checkout

Robisz przelewy przez internet? Bardzo dobrze. To znaczy, że korzystasz z dobrodziejstw bankowości internetowej. Ale pewnie denerwuje cię każdorazowe wpisywanie loginu i hasła do systemu, a potem jeszcze kolejne wpisywanie

JESZCZE NIE PŁACIŁEŚ!

PŁATNOŚCI I BANKOWOŚCI ELEKTRONICZNEJ

hasła SMS-owego przy wykonaniu każdej akcji? Koszmar zaczyna się w momencie, kiedy robisz zakupy online i za każdym razem musisz wpisywać swoje dane z miejscem dostawy. Denerwuje cię to? Mamy dla ciebie świetne rozwiązanie. Masterpass to rodzaj portfela internetowego, w którym możesz trzymać swoje pieniądze i dokonywać szybkich operacji, kiedy tylko chcesz i gdziekolwiek jesteś. Wystarczy, że zalogujesz się raz, przypiszesz do systemu dowolną kartę płatniczą MasterCard i zatwierdzisz transakcję kodem PIN. Na uwagę zasługuje fakt, że w ten sposób możesz płacić za zakupy w sieci i w sklepach stacjonarnych, które obsługują płatności Masterpass.

To bezpieczny i szybki sposób płatności. Najważniejsze zalety to brak konieczności wpisywania swoich danych i adresu przy płatnościach online oraz uczestnictwo w systemie partnerskim, który daje dostęp do interesujących promocji w wybranych sklepach.

Bliźniaczą opcją jest Visa Checkout, która działa z kartami Visa.

Selfie Pay

Selfie Pay to opcja, która na pierwszy rzut oka wygląda bardzo abstrakcyjnie. Wyobrażasz sobie płatności z wykorzystywaniem własnego zdjęcia? Robisz zakupy w sklepie, a na koniec… robisz sobie fotkę! Właśnie tak działa zaprezentowana w 2016 roku usługa MasterCard. Operator transakcji wyszedł naprzeciw oczekiwaniom maniaków portali społecznościowych i uruchomił całkiem ciekawą usługę, która ma spore szanse na sukces.

Wyobraź sobie, że robisz dowolne zakupy i chcesz za nie zapłacić. Standardowo musiałbyś wpisać swoje dane, wybrać sposób płatności i podać kod SMS. Selfie Pay wyklucza podawanie haseł, które już w oficjalnym oświadczeniu z początku roku zostały skrytykowane przez gigantów świata IT, w tym Microsoft i Google. Apple przecież z dumą ogłaszało funkcję odblokowywania telefonów „za pomocą twarzy" – wystarczyło spojrzeć w przedni obiektyw i konieczność wpisywania PIN-u znikała. Podobnie działa Selfie Pay. Potwierdzeniem operacji jest twoja twarz. Po dokonaniu zakupów system zamiast poprosić o niewygodne wpisanie hasła do bankowości poprosi cię o zrobienie sobie aktualnej fotki.

Metoda ta polega na potwierdzeniu transakcji poprzez rozpoznanie kształtu twarzy użytkownika. MasterCard coraz śmielej promuje swój pomysł na całym świecie. Opcja jest szerzej testowana w USA, Kanadzie i Holandii. W tym roku taką możliwość dostali Rosjanie. Całkiem możliwe, że niebawem Selfie Pay wejdzie również i do Polski.

Czy to bezpieczne? Aby nie powtarzać błędów pierwszych iPhone'ów z „funkcją odblokowywania twarzą", którą dało się oszukać podstawieniem zdjęcia, MasterCard wykorzystuje biometrię twarzy. Użytkownicy Selfie Pay w ramach bezpieczeństwa są proszeni o wykonanie pewnych gestów, w tym zrobienie niesławnego „dzióbka".

Płatności odciskiem palca lub skanem siatkówki oka

To nie jest wizja rodem z filmu science fiction. Już teraz trwają testy płatności oparte na biometrycznej technologii palm vein, która identyfikuje klienta po zeskanowaniu naczyń krwionośnych jego dłoni, układu siatkówki oka czy odcisku palca. Po zarejestrowaniu wzoru w bankomacie lub specjalnym terminalu POS płacący będzie musiał powiązać go z numerem swojej karty płatniczej i gotowe. Technologia ta jest dostępna w Polsce. Skorzystamy z niej między innymi w bankomatach Planet Cash.

Czy to koniec stania w kolejce do kasy i noszenia gotówki?

Zakupy bez konieczności posiadania gotówki czy stania w kolejce do kasy obsługiwanej przez człowieka to stosunkowa nowość. Teraz takie rozwiązanie pojawi się także w naszym kraju. Pierwszy program tego typu nie jest rozwiązaniem testowym. Będzie wdrażane ono normalnie we wszystkich sklepach pewnej sieci marketów.

Po raz pierwszy w Polsce będziemy mogli zrobić zakupy bez gotówki oraz karty bankowej. Do opłaty wystarczy specjalna aplikacja oraz smartfon. Program **Skanuj i kupuj** uruchomiony jest przez sieć supermarketów Piotr i Paweł. Wszystkich operacji związanych z płatnościami będziemy dokonywać wyłącznie w specjalnej aplikacji.

Na razie program Skanuj i kupuj pojawi się w sześciu sklepach sieci. Będzie to sklep w Poznaniu (ul. Gronowa 18), we Wrocławiu (w Sky Tower), w Markach pod Warszawą (ul. Piłsudskiego 200A) oraz dwa sklepy warszawskie (ul. Stawki 2A oraz w CH Blue City). W ciągu kilku miesięcy możliwość kupowania smartfonem ma pojawić się we wszystkich sklepach sieci. Podobne systemy testowane są także za granicą, na przykład w USA. W Polsce pilotażowy program tego typu zaczęła na przykład sieć Tesco, nad taką formą zakupów myśli także Carrefour. Zakupy wykonamy dowolnym smartfonem.

Aby dokonać takich nowoczesnych zakupów, trzeba będzie zainstalować na swoim smartfonie odpowiednią aplikację i powiązać ją z kartą bankową. Potem wystarczy skanować kody kreskowe wszystkich towarów, które wrzucamy do koszyka. Po zakończeniu dokonujemy płatności w kasie samoobsługowej albo w aplikacji. W sklepie będzie wyznaczona specjalna strefa kupna, ponieważ musimy mieć możliwość otrzymania paragonu. Do tego system będzie wyznaczał losowych klientów do kontroli tego, czy zgadza się zawartość koszyka z paragonem.

Fot. Vikayatskina, Prykhodov, Andriy Popov/123rf.com

DOKĄD ZMIERZAJĄ NOWOCZESNE METODY PŁATNOŚCI?

Bankowość elektroniczna rozwija się w zastraszającym tempie. Jeszcze do niedawna przełomem było płacenie kartami w internecie, a dziś możemy płacić i bez tego, wystarczy zrobienie sobie selfie. Niezależnie od metody dokonywania płatności widać w nich kilka wspólnych mianowników. Wszystkie dążą do tego, aby maksymalnie ułatwić nam możliwość płacenia i ostatecznie pożegnać się z gotówką. Dziś już nawet nie musimy mieć przy sobie karty płatniczej czy telefonu, aby zapłacić za zakupy – w niektórych miejscach wystarczy potwierdzenie odciskiem palca!

TO MUSISZ WIEDZIEĆ O BLIKU NUMER KONTA

BLIK to wyjątkowe w skali światowej rozwiązanie. *Pozwala na wypłaty z bankomatów bez karty płatniczej oraz przelewy do dowolnych osób – wystarczy, że znamy numer telefonu odbiorcy naszego przelewu. Co jeszcze warto wiedzieć o płatnościach BLIK?*

Dziś nie potrzebujemy już znać numeru konta odbiorcy, aby przesłać mu pieniądze. Wystarczy numer telefonu. To bardzo szybkie i proste rozwiązanie, a co najważniejsze, przelewy na telefon są darmowe. Sprawdzi się ono w każdej sytuacji, wystarczy mieć aplikację mobilną banku i zarejestrować swój numer telefonu w usłudze. Taka możliwość pojawiła się w ofercie naszych polskich banków już parę lat temu, jednak dopiero po stworzeniu schematu BLIK zaczęto szerzej korzystać z tej metody. Polskiemu Standardowi Płatności zawdzięczamy stworzenie bazy danych, która zawiera numery telefonów z numerami osób biorących udział w projekcie. Co musisz wiedzieć o BLIK-u i jak z niego korzystać?

JAK ZACZĄĆ UŻYWAĆ BLIK-A?

Najpierw należy zainstalować aplikację mobilną swojego banku, aktywować funkcję BLIK oraz ustalić limity transakcji.

W jaki sposób płacić BLIK-iem? Wszelkie transakcje wykonywane poprzez BLIK można zrealizować w bardzo łatwy sposób. Wystarczy kilka kroków:

- Wejdź do aplikacji swojego banku i wybierz BLIK.
- Następnie wygeneruj kod składający się z sześciu cyfr. Jest on ważny jedynie przez dwie minuty, należy go wpisać w terminalu płatniczym.
- Dostaniesz informację na telefon o kwocie i miejscu transakcji i musisz ją potwierdzić.
- Po ukończeniu zlecenia dostaniesz paragon oraz wydruk potwierdzający przelew.

Jak płacić wygodnie przez BLIK

BLIK jest systemem płatności mobilnych i za jego pomocą można wykonywać transakcje w takich miejscach, jak punkty usługowo-handlowe oraz w internecie. Można również wypłacać pieniądze z bankomatu oraz przelewać środki na inne rachunki, do odbiorców, którzy także są zarejestrowani w usłudze. Chcąc skorzystać z BLIK-a, nie trzeba mieć bardzo nowoczesnego urządzenia – wystarczy podstawowy smartfon i aplikacja mobilna swojego banku (musi on współpracować z systemem BLIK). Telefon może nie mieć modułu NFC, potrzebny on jest jedynie przy płatnościach zbliżeniowych.

Duża liczba współpracujących instytucji finansowych to jednak dopiero połowa sukcesu. Inną ważną kwestią jest to, gdzie BLIK-iem zapłacimy. W tym momencie stacjonarnych punktów wspierających standard jest w Polsce czterdzieści kilka tysięcy. Polski Standard Płatności podpisał także umowy z integratorami internetowymi DotPay i PayPro – dzięki temu już teraz możemy płaci BLIK-iem w ponad 5000 sklepach internetowych.

Twórcy zapewniają, że cała infrastruktura będzie rozwijać się bardzo szybko i że w ciągu kilku miesięcy uda się osiągnąć ponad 150 tysięcy wspierających BLIK terminali. Obecnie system obejmuje zasięgiem około 60 procent wszystkich klientów polskich banków. PSP zamierza w niedalekiej przyszłości wprowadzić także możliwość robienia błyskawicznych przelewów pomiędzy dwoma telefonami. Brzmi nieźle i ma szansę się upowszechnić. Wymagania co do telefonu są bardzo niskie – proces płatności nie wymaga modułu NFC, gdyż system działa na innej zasadzie. Jakiej? Komputer Świat przygotował krótki przewodnik, z którego dowiecie się, jak płacić w sklepach, korzystać z bankomatu i z systemu czeków w technologii BLIK.

CZY TELEFONU?

Wypłata pieniędzy z bankomatu za pomocą telefonu. Jak to zrobić?

Wypłata pieniędzy z bankomatu wygląda podobnie jak płatności. Najpierw w bankomacie wybierz odpowiednią opcję, aby wypłacić pieniądze, po czym wprowadź kwotę. Następnie wejdź do aplikacji i wybierz BLIK, który wygeneruje kod. Otrzymany kod wprowadź w bankomacie i potwierdź całą transakcję na telefonie.

Gdzie można zapłacić przy wykorzystaniu BLIK-a?

Największą zaletą BLIK-a jest fakt, że współpracuje on z wieloma bankami w Polsce – między innymi: Alior Bank, Bank Millennium, Santander Bank Polska, ING Bank Śląski, mBank, PKO BP i Inteligo. Liczba udziałowców stale się powiększa i niedługo z nowego standardu skorzystają także klienci między innymi: Getin Bank, Eurobank, NeoBank, BNP Paribas Bank Polska, Credit Agricole i Idea Bank.

Gdzie można zapłacić przy wykorzystaniu BLIK-a? Przede wszystkim w punktach oznaczonych logo BLIK-a, sklepach stacji Orlen i stacji Shell. Najlepiej wejść w wyszukiwarkę BLIK, gdzie znajduje się lista miejsc umożliwiających płacenie za pomocą tego typu płatności.

W jakich bankomatach można wypłacić pieniądze z pomocą tego systemu? Taką możliwość dają bankomaty Millennium, PKO BP, Santander Bank Polska, Euronet, ING Bank Śląski, Alior Bank, Credit Agricole, Getin Bank, Idea Bank, mBank. W 11 tysiącach miejsc w całym kraju można skorzystać z takiej metody wypłacania pieniędzy.

W JAKICH BANKACH W POLSCE DZIAŁAJĄ PRZELEWY NA TELEFON?

W systemie BLIK uczestniczą największe banki w Polsce, a w tym:

- Alior Bank – aplikacja Alior Mobile
- Bank Millennium – aplikacja Bank Millennium
- Santander Bank Polska – aplikacja Santander mobile
- ING Bank Śląski – aplikacja Moje ING Mobile
- Inteligo – aplikacja IKO
- mBank – aplikacja mBank PL
- Kompakt Finanse – aplikacja Kompakt Finanse (dawniej Orange Finanse)
- PKO Bank Polski – aplikacja IKO

W tych instytucjach można wykonać transakcje z wykorzystaniem systemu BLIK. Do programu nie należą natomiast banki Getin Bank i T-Mobile Usługi Bankowe. W trakcie wprowadzania usługi jest BGŻ BNP Paribas i Raiffeisen Polbank.

Warto wiedzieć, że Elixir Express jest systemem, który obsługuje wszelkie przelewy BLIK, w przeciwieństwie do innych tradycyjnych przekazów, transakcje za pomocą tego systemu są w pełni darmowe. Plusem jest to, że aby wykonać przelew, nie trzeba wpisywać sporej ilości danych, takich jak nazwisko, imię, adres, numer rachunku bankowego, wystarczy tylko wybrać daną osobę z kontaktów w telefonie. Dzięki temu skraca się czas wykonania transakcji.

Przelewy na numery telefonu w bazie BLIK

Chcesz przelewać komuś pieniądze? Nie trzeba podawać numeru konta, wystarczy jedynie wpisać numer telefonu odbiorcy. Pieniądze szybko do niego trafią, o ile uczestniczy w programie BLIK.

W jaki sposób wykonać przelew? Dyspozycję płatności wystarczy złożyć w aplikacji mobilnej banku, tam gdzie przeważnie zlecasz tradycyjne przelewy albo tam, gdzie generujesz kod BLIK. Musisz podać numer swojego kontrahenta, wpisać kwotę, po czym zatwierdzić całą transakcję. Zlecając przelewy na telefon z systemem BLIK, nie musisz mieć zarejestrowanego numeru. Jednak jeśli ktoś wykona tą metodą przelew do ciebie, możesz go nie dostać.

Czy opłaca się aktywować BLIK?

Na pewno warto dać mu szansę i aktywować możliwość płatności na telefon. BLIK przydaje się zwłaszcza w nagłych i awaryjnych sytuacjach, na przykład jeśli zapomnimy wziąć ze sobą portfel i nie mamy jak zapłacić. Telefon da nam dostęp do naszych pieniędzy również w przypadku, gdy nasze karty płatnicze zostaną skradzione. Telefon mamy niemal zawsze przy sobie, więc posiadając aktywowany BLIK, będziemy mogli w każdej chwili wykonać szybki przelew.

Bezpieczeństwo płacenia telefonem

Bezpieczeństwo wykonywania przelewów przez telefon jest o wiele wyższe niż w przypadku tradycyjnych rodzajów płatności. Przede wszystkim dlatego, że generowany kod, składający się z sześciu cyfr, jest ważny tylko przez 120 sekund, przez co osoba, która mogłaby go podejrzeć, będzie miała bardzo krótki czas na użycie go. Jest to duża zaleta tego systemu. Karta płatnicza niesie ze sobą również niebezpieczeństwo zeskanowania jej, natomiast podejrzany kod BLIK nie przyniesie żadnych korzyści przestępcy. Dobrym zabezpieczeniem jest również wprowadzenie potwierdzeń za każdym razem, gdy będziemy chcieli wykonać operację na kwotę powyżej 50 złotych. Mniejsze kwoty także musisz potwierdzić telefonem, jednak nie wpisujesz za każdym razem kodu.

Technologie NFC i HCE w służbie bankowości elektronicznej

NFC to technologia, z której również często korzysta się przy płatnościach mobilnych. Przy płatności NFC bank musi dać swojemu klientowi wirtualną kartę do jego konta osobistego, następnie jest ona zapamiętywana na karcie SIM smartfona. Klient korzysta ze specjalnej aplikacji w telefonie i karty SIM, po czym może płacić zbliżeniowo przez swoje urządzenie.

HCE polega na zainstalowaniu aplikacji mobilnej banku w telefonie, a następnie na dodanie do niego karty płatniczej. Minusem tej technologii jest to, że działa jedynie na Androidzie i w dodatku tylko na jego nowszych wersjach. Posiadacze urządzeń z jabłkiem w logo niestety muszą obejść się smakiem. Telefon obsługujący tę metodę płatności musi także obsługiwać technologię zbliżeniową NFC.

Przelew na telefon z systemem BLIK – maksymalny przelew oraz dobowe limity

W celu zwiększenia bezpieczeństwa banki wprowadzają dzienne limity operacji oraz limity jednorazowych transakcji. Jak to wygląda w przykładowych bankach?

- **Bank Millennium** – 500 zł dziennie, można wykonać dowolną ilość przelewów w ciągu doby.
- **Santander Bank Polska** – w ciągu doby można przelać maksymalnie 3000 złotych.
- **Alior Bank** – 500 zł w ciągu doby, można przelać maksymalnie 5000 złotych, a w ciągu miesiąca 30 000 złotych.
- **Inteligo** – 1000 zł w ciągu doby, można wykonać 20 transakcji w ciągu doby, limit można ustalić samodzielnie.
- **ING Bank Śląski** – 200 zł w ciągu doby, można zrobić przelew na maksymalnie 500 zł.

W końcu powstał w Polsce jednolity i spójny system płatności na miarę XXI wieku. Karta płatnicza nie jest już potrzebna! Warto korzystać z BLIK-a. To wygodna i bezpieczna metoda.

RAPORT
bankowość elektroniczna

CZY BANKOWOŚĆ JEST BEZPIECZNA

Hakerzy chętnie by weszli w ***posiadanie naszych danych dostępowych do kont bankowych.*** *Z jakich metod korzystają cyberprzestępcy, by tego dokonać? Na co zwracać uwagę, by nie paść ofiarą złodziei w sieci?*

Czy bankowość elektroniczna jest bezpieczna? To pytanie zadaje sobie wielu z nas. Zdalne płatności budzą sporo obaw co do bezpieczeństwa. Czy słusznie? Ten artykuł przedstawia podstawowe zasady bezpiecznego kupowania w sieci, mechanizmy zabezpieczające i najczęściej występujące zagrożenia.

Wygoda a przezorność w bankowości elektronicznej

Gotówka, jakkolwiek miła w dotyku i niezmiennie pożądana przez wszystkich, w coraz większym stopniu zastępowana jest przez inne formy przekazywania środków finansowych. U nas jeszcze nie w takim tempie jak w innych krajach (Szwedzi poważnie przymierzają się do całkowitego zlikwidowania pieniądza papierowego i przejścia na transakcje elektroniczne, podobne zamiary zdradzają też Duńczycy), ale i tak obrót bezgotówkowy stale zyskuje w Polsce popularność. I nic dziwnego: elektroniczne płatności umożliwiają szybkie i wygodne zakupy, zarówno gdy płacimy zbliżeniowo kartą w sklepie stacjonarnym, jak i podczas zamawiania towarów przez internet. Polski rynek e-commerce ma pod koniec bieżącego roku osiągnąć wartość 38,5 miliarda złotych, a liczba rodzimych sklepów internetowych przekroczyć ma 23 tysiące. Warto zatem zapoznać się z różnymi sposobami płacenia bez użycia monet i banknotów.

Bankowość elektroniczna jest wyjątkowo wygodna, jednak trzeba zachować pewne zasady i być świadomym zagrożeń. Klienci nie analizują tematu bezpieczeństwa, co nie musi wynikać z pełnego zaufania do banków, ale chociażby z obaw przed uznaniem za człowieka nienadążającego za rozwojem technologii. Ludziom korzystającym już jakiś czas z bankowości online niezmiernie trudno byłoby zmienić swoje przyzwyczajenia.

To wszystko nie musi jednak oznaczać, że korzystanie z usług finansowych za pośrednictwem internetu zawsze jest niebezpieczne. Warto po prostu znać zagrożenia i mieć świadomość, że nie wystarczy ciągłe ulepszanie technologii zabezpieczeń przez bank. Część odpowiedzialności w naturalny sposób spoczywa również na klientach.

Zagrożenia:

Wirusy

Podstawowym zagrożeniem, charakterystycznym nie tylko dla bankowości elektronicznej, są wirusy. Złośliwe oprogramowanie w różnej postaci ma jeden model działania. Polega on na przejęciu kontroli nad komputerem ofiary bez jej zgody i świadomości. W ten sposób przestępcy najczęściej wykradają dane niezbędne do zalogowania do konta. Mogą wtedy dokonywać dowolnych transakcji. Trzeba pamiętać, że zaatakowane może zostać każde urządzenie, z którego korzysta się z bankowości internetowej. Oprócz chronionego antywirusem komputera może to być na przykład smartfon lub tablet.

Internetowi oszuści chętnie korzystają też z wirusów, które przechwytują wpisywane przez nas informacje. Zdarzały się nawet przypadki trojanów, które „wyczuwały", że odwiedzamy stronę banku i wpisujemy numer konta do przelewu, a następnie niepostrzeżenie podmieniały go na inny, należący do elektronicznych rzezimieszków. Aby nie paść ich łupem, należy wystrzegać się instalowania oprogramowania z nieznanych źródeł, a szczególnie z wyskakujących podczas przeglądania internetu okienek natarczywie żądających od nas instalacji jakiejś aplikacji. Do szczególnie ulubionych przez e-złoczyńców metod należy straszenie nas hasłem „UWAGA WIRUS! – kliknij tutaj, by wyczyścić swój system". Kliknięcie nie czyści systemu, lecz właś nie wprowadza do niego wirusa. Takie fałszywe ostrzeżenie szczególnie często pojawia się na smartfonach, ale użytkownicy komputerów stacjonarnych też nie są bezpieczni. Jeśli często trafiamy na takie komunikaty, warto rozważyć skorzystanie z zaufanych programów antywirusowych.

Phishing

Phishing to metoda oszustwa opierająca się na podawaniu się za bank i podstępnym uzyskiwaniu w ten sposób danych potrzebnych do kontroli nad kontem. Oszuści wysyłają maile, dbając o to, żeby treść do złudzenia przypominała szatę graficzną banku, w którym potencjalna ofiara ma konto. Adres, z którego wysyłane są takie wiadomości, również ma wyglądać jak najbardziej autentycznie. Złodzieje proszą o przesłanie loginu i hasła lub zalogowanie się do systemu poprzez podany link w celu wykonania jakiejś czynności. W pierwszym przypadku pretekstem może być na przykład konieczność potwierdzenia autentyczności adresu e-mail użytkownika dla potrzeb aktualizacji danych. Druga metoda jest bardziej skomplikowana, wymaga większych nakładów oraz nie jest podejrzane na pierwszy rzut oka. Tutaj oszuści proszą o samodzielne zalogowanie się na stronie banku, aby na przykład rutynowo zmienić hasło ze względów bezpieczeństwa. Podają przy tym w wiadomości link do strony. Tutaj tkwi sedno oszustwa. Strona jest stworzona przez samych oszustów, jej adres różni się na przykład jedną literą, natomiast szata graficzna i interfejs są niemal identyczne. Po próbie zalogowania złodzieje jako administratorzy strony mają login i hasło, którego mogą użyć do wyprowadzenia pieniędzy.

Ć ELEKTRONICZNA A?

Pozyskanie danych osobowych

Ta metoda jest najbardziej niebezpieczna, ponieważ żeby się przed nią ochronić, nie wystarczy ostrożność i zdrowy rozsądek oraz dobre oprogramowanie antywirusowe. Dziś jeśli znamy odpowiednie dane osobowe, możemy za kogoś założyć konto lub zaciągnąć kredyt. Nieostrożne podawanie informacji o sobie może zostać użyte przez złodziei. O oszustwie ofiara dowiaduje się najczęściej jakiś czas po nim. Niestety, to na zaatakowanym będzie spoczywał faktyczny ciężar udowodnienia, że to przestępca, a nie on sam dokonał określonych czynności. Często prowadzi to w ostateczności do tego, że okradziony musi spłacić wszystkie zobowiązania.

Zakupy w internecie

Ta metoda pośrednio związana jest z bankowością elektroniczną. Do jej zastosowania nie trzeba bowiem ingerować w proces przesyłania danych, niepotrzebna jest też wiedza informatyczna. Trzeba jedynie wystawić ofertę sprzedaży przez internet. Może łączyć się to z założeniem strony internetowej sklepu, wystarczy jednak oferta od osoby prywatnej na jakimkolwiek portalu z ogłoszeniami. Po dokonaniu płatności oszust po prostu znika, nie odzywa się lub wysyła paczkę bez zakupionej zawartości. Choć nie wiąże się to bezpośrednio z technologią bankowości online, to bazuje na powszechności zakupów internetowych, które przy jej pomocy znacząco zyskały na popularności.

Jak o bezpieczeństwo dbają banki?

Banki stawiają przede wszystkim na działania prewencyjne. Tworzą one specjalne systemy, które monitorują klientów. Po pierwsze sprawdzają, czy nie pojawiło się u nich szkodliwe oprogramowanie. Po drugie analizują samo zachowanie klienta w poszukiwaniu niepokojących praktyk. Na przykład korzystający z polskiego banku, logujący się zawsze z Rzeszowa, używa przelewów internetowych do opłacania bieżących rachunków, po czym nagle wypłaca całe oszczędności z komputera znajdującego się w Uzbekistanie. Sytuacja z tego skrajnego przykładu wzmogłaby czujność banku, a nawet mogłaby doprowadzić do zablokowania transakcji.
W odpowiedzi na phishing wszystkie banki jasno deklarują, że nigdy nie proszą za pośrednictwem maili o żadne dane. Podobnie nigdy nie jest wymagane zalogowanie się poprzez konkretny link wskazany w wiadomości.
Znaczna część banków wymaga potwierdzenia transakcji kodem SMS. Zabezpieczenie to można wyłączyć dopiero po dodaniu odbiorcy do listy zaufanych, która to czynność i tak musi być potwierdzona tą samą drogą. Oprócz tego często domyślnie ustawiany jest limit dziennych transakcji oraz wypłat z bankomatu. Standardem jest natomiast szyfrowanie przekazywania danych na stronie internetowej banku.

O czym powinien pamiętać klient?

Przede wszystkim trzeba zacząć od stwierdzenia, które może brzmieć jak banał. Korzystający z bankowości internetowej powinien po prostu zachowywać ostrożność. Nawet najlepsze zabezpieczenia ze strony banku nie wystarczą, jeśli oszuści będą mogli liczyć na naiwność swoich ofiar.
Pierwszym krokiem może być zadbanie o odpowiednie zabezpieczenie antywirusowe. To powinno zapewnić ochronę przed złośliwym oprogramowaniem. Konieczne jest jednak, aby pamiętać o wszystkich urządzeniach, które wykorzystywane są do logowania na stronie banku lub przez aplikację. Zależnie od systemu operacyjnego, smartfony i tablety wymagają różnej ochrony, uniwersalną radą jest natomiast unikanie instalowania aplikacji niewiadomego pochodzenia.
Do obrony przed phishingiem wystarczy mieć świadomość takiego zagrożenia i pamiętać, że banki nigdy nie proszą o podawanie danych drogą mailową, a logować należy się zawsze przez stronę banku, a nie jakiekolwiek linki z wiadomości. Dla pełni bezpieczeństwa można jeszcze zawsze sprawdzać adres witryny, szczególnie jego początek. Powinien on zaczynać się od „https", co oznacza połączenie szyfrowane. Najlepiej zachować weryfikację transakcji kodem SMS oraz limity wypłat, zdejmując je tylko w razie potrzeby dokonania większych transakcji. Hasło powinno być regularnie zmieniane i mocne. Istnieje wiele narzędzi, które powiedzą ci, czy twoje hasło jest bezpieczne, czy też nie. Możesz to sprawdzić przez aplikację internetową **The Password Meter**. Wystarczy, że wpiszesz swoje hasło i zobaczysz jego mocne i słabe punkty.
Skrajnie niebezpieczne jest używanie na daty urodzenia, swojej lub kogoś bliskiego. Warto regularnie sprawdzać historię transakcji, ponieważ czasem oszuści kradną małe kwoty od wielu osób, zakładając, że ubytki niewielkich sum nie zwrócą ich uwagi.
Kolejne rady dotyczą nie tylko bankowości elektronicznej, ale też innych sfer życia. Po pierwsze, należy pilnować swoich danych osobowych i wylogowywać się zaraz po dokonaniu operacji na komputerze, do którego ktokolwiek niezaufany może mieć dostęp. Dobrze, unikać wykorzystywania do tego otwartych sieci internetowych.

BANKOWOŚĆ ELEKTRONICZNA MOŻE BYĆ BEZPIECZNA

Istnienie wyżej opisanych metod oszustwa wcale nie oznacza, że nie da się bezpiecznie korzystać z bankowości online. Przestępczość pojawia się wszędzie tam, gdzie są pieniądze. Czy noszenie przy sobie dużej ilości gotówki niesie ze sobą mniejsze ryzyko niż posiadanie na smartfonie aplikacji do bankowości mobilnej? Grunt to znać wszystkie zagrożenia i ich mechanizmy, zachowywać czujność, a przedstawione w tekście porady przekuć w nawyk.

Fot. Bloomua, Le Moal Olivier, Galina Peshkova/123rf.com

RAPORT
bankowość elektroniczna

BĄDŹ BEZPIECZNY W BANKOWOŚCI

NA CO POLUJ

*Dziś trudno wyobrazić sobie dzień bez sprawdzenia poczty elektronicznej i serwisów społecznościowych oraz innych portali. Ten popularny trend objął także bankowość – **elektroniczny dostęp do rachunku jest podstawą naszej codzienności, bez której bardzo trudno żyć**. Niestety, rozwój e-bankowości, bankowości mobilnej i kart płatniczych spowodował pojawienie się różnych przestępstw, związanych z internetowym dostępem do naszych danych osobowych i pieniędzy. Zobaczcie, na co polują nowocześni oszuści*

Na współczesnego człowieka czyha bardzo dużo zagrożeń związanych z bankowością elektroniczną. Do najważniejszych należą:

Wyłudzanie danych (czyli tak zwany phishing)
To metoda, która polega na podszywaniu się przestępcy pod bank celem wyłudzenia od klienta pożądanych informacji albo nakłonienia go do określonych działań. Haker chce poznać nasze loginy i hasła. Aby osiągnąć cel, przestępcy wysyłają do klientów fałszywe maile albo dzwonią do ofiar, podszywając się pod pracowników banku – proszą nas o pozostawienie danych do bankowości elektronicznej lub kliknięcie na link podesłany w wiadomości e-mail. Jeżeli będziemy nieostrożni, haker pozna login oraz hasło do naszego konta, a następnie wyczyści rachunki z pieniędzy.

Złośliwe oprogramowanie
Zainstalowanie na komputerze wirusów albo programów szpiegujących, których celem jest śledzenie informacji pojawiających się na ekranie komputera, w tym znaków wprowadzanych na klawiaturze, a nawet przejmowanie kontroli nad urządzeniem to jedna z podstawowych metod działania cyberprzestępców. Jak można zarazić się takim wirusem? Często przestępcy wysyłają do klientów fałszywe e-maile, w których załączone jest złośliwe oprogramowanie. Jeśli nasz komputer nie jest zabezpieczony i otworzymy taką wiadomość, wtedy narażamy się na duże niebezpieczeństwo.

Kopiowanie kart płatniczych (czyli skimming)
Skimming to kopiowanie danych znajdujących się na pasku magnetycznym karty płatniczej w momencie korzystania z bankomatu. Przestępca instaluje specjalną nakładkę w otworze, w którym umieszczamy kartę, i poprzez to wykrada wszystkie dane zapisane na pasku magnetycznym. PIN może zostać poznany dzięki malutkim kamerom umieszczonym nad klawiaturą bankomatu.

Zakupy i płatności internetowe
Zakupy przez internet bywają ryzykowne. Jeżeli kupujemy coś w nieznanych e-sklepach, możemy stracić pieniądze za zakupiony towar oraz stracić środki zgromadzone na koncie (złośliwe oprogramowanie przechwyci dane z karty i haker dokona zakupów na nasz rachunek). Powstaje pytanie, czy skoro sprzedawcy dysponują naszymi danymi, to nie mogą one paść łupem cyberprzestępców? Często bowiem słyszymy o wyciekach danych kart, i zdarzają się one nawet największym: w 2011 roku miał miejsce ogromny atak na bazę PlayStation Network, gdzie wyciekły szczegóły milionów kont. W zeszłym roku złodzieje skradli dane kart tysięcy gości amerykańskich hoteli z sieci Hyatt, Hilton, a także należących do Donalda Trumpa. Wciąż zdarzają się też indywidualne przypadki kradzieży informacji o karcie, na przykład poprzez nakładki na bankomaty bądź automaty płatnicze czy za sprawą phishingu. Nie ma się jednak czego specjalnie obawiać, te zdarzenia bowiem stanowią margines ogromu transakcji dokonywanych na całym świecie, podobnie jak kradzieże kieszonkowe i rabunki zdarzają się, ale nie na tyle często, by należało zrezygnować z noszenia portfela. A przede wszystkim użytkowników kart chroni przed stratami tak zwany chargeback.

Aplikacje mobilne są dziś bardzo popularne
Telefon, jeśli nie jest odpowiednio zabezpieczony (poprzez instalację niezaufanych aplikacji), może zostać wykorzystany przez hakera do przechwycenia programów do bankowości mobilnej. Wielu z nas korzysta z takich aplikacji, a to daje przestępcom duże pole manewru.

Karty zbliżeniowe
To łakomy kąsek dla złodziei ze względu na płatności bez użycia PIN-u. Przestępcy mogą dokonać wielu transakcji (każda do 50 zł) i czują się bezkarni – dokonują zakupu bez pokazywania karty sprzedawcy, który mógłby zweryfikować ich tożsamość.

Kradzież tożsamości
To poważny problem. Nasze dane osobowe to bardzo cenna informacja dla przestępcy. Z ich pomocą można na przykład założyć konto w banku czy wziąć kredyt. Ludzie często lekkomyślnie podają takie dane w miejscach publicznych, a przy tym nie zwracają uwagi na to, że ktoś może to usłyszeć i wykorzystać do oszustwa.
W 2012 roku na portalach społecznościowych wybuchła dziwaczna epidemia: młodzi ludzie

ELEKTRONICZNEJ Ą ZŁODZIEJE?

zaczęli wrzucać do sieci zdjęcia swoich kart kredytowych, żeby pochwalić się przed znajomymi posiadaniem tego nobilitującego ich zdaniem przedmiotu. Zamieszczano obrazy przedstawiające zarówno awers, z nazwiskiem właściciela, numerem karty i datą jej ważności, jak i rewers, gdzie znajduje się numer zabezpieczający. Te dane w zupełności wystarczą, aby dokonać zdalnego zakupu. Nie wiadomo, ile osób straciło w ten sposób pieniądze, ale sytuacja zwróciła powszechną uwagę na fakt, że złodzieje mogą przeszukiwać sieć w poszukiwaniu właśnie takich danych, a potem bez skrupułów z nich korzystać.

Zasady bezpieczeństwa

Metody oszukiwania mogą budzić niepokój. Warto jednak zdawać sobie sprawę z tego, że nasze dane osobowe oraz konta bankowe mogą zostać nielegalnie wykorzystane. Nie jesteśmy jednak na straconej pozycji. Możemy chronić nasz rachunek i dane osobowe. Kilka prostych rad może ochronić twoje pieniądze. Przede wszystkim:

1 Nie podawaj danych logowania do bankowości przez e-mail lub telefon – bank nigdy nie prosi klienta o login czy hasło do konta. Jeżeli podamy nasze dane do logowania do rachunku bankowego, to możemy być pewni, że złodziej to wykorzysta.

2 Zabezpieczaj komputer oraz telefon – urządzenia, na których korzystasz z rachunku bankowego, muszą być chronione poprzez: legalne oprogramowanie, które jest okresowo aktualizowane, programy antywirusowe oraz firewall (czyli zaporę sieciową), która chroni przed atakami z zewnątrz.

3 Nie otwieraj podejrzanych e-maili i załączników – jeśli masz wątpliwości co do pochodzenia e-maila, oznacz go jako spam i usuń.

4 Sprawdzaj zabezpieczenia strony banku – podczas logowania do konta zwróć uwagę na dwa elementy – są to szyfrowane połączenia oraz certyfikat bezpieczeństwa. Połączenia szyfrowane możesz rozpoznać po symbolu kłódki w pasku adresu przeglądarki i „https" na początku adresu do logowanej strony. To gwarantuje, że twoje dane są bezpieczne. Certyfikat potwierdza, że strona jest zaufana. Możemy go sprawdzić, klikając na kłódkę obok adresu witryny.

5 Sprawdzaj datę ostatniego logowania – warto zwrócić uwagę na tę informację i zweryfikować, czy faktycznie wtedy korzystaliśmy z konta.

6 Stwórz silne hasło do bankowości. Musi być unikalne, odpowiednio długie i składać się z wielkich i małych liter oraz cyfr i znaków specjalnych, takich jak #, %, @.

7 Zawsze weryfikuj kod SMS – jeśli haker poznał twój numer telefonu, może podmienić wiadomości z banku. Czytaj dokładnie takie SMS-y oraz sprawdzaj, czy zgadza się kwota operacji i numer rachunku odbiorcy.

8 Korzystaj z bezpiecznych sieci Wi-Fi – logowanie się do banku poprzez otwarte sieci (na przykład te w galeriach handlowych) to duże ryzyko. Brak jakichkolwiek zabezpieczeń to bardzo łatwy cel dla hakerów.

9 Sprawdzaj bankomaty – karty płatnicze mogą być skopiowane przez hakerów. W celu uniknięcia nieprzyjemności przyjrzyj się maszynie, z której wypłacasz pieniądze. Twoją czujność muszą wzbudzić nietypowe elementy, takie jak na przykład odstające części obudowy lub miniaturowe kamery.

10 Włącz powiadomienia SMS – wiadomości SMS od banku z informacją o zmianach na rachunku często są płatne, jednak warto włączyć taką usługę, aby mieć kontrolę nad rachunkiem.

11 Ustaw limity dla transakcji kartami płatniczymi – wysokie limity dla kart debetowych czy kredytowych ułatwiają złodziejom zerowanie naszych kont. Aby tego uniknąć, warto zmienić maksymalne wartości dziennych wypłat na niższe.

12 Dbaj o swój telefon – jeśli nie będzie odpowiednio zabezpieczony, a aplikacje niezaktualizowane, złodziej przejmie kontrolę nie tylko nad urządzeniem, ale także wykorzysta je i ogołoci konto bankowe.

13 Kontaktuj się z bankiem w razie potrzeby – jeśli podczas korzystania z internetu i konta bankowego coś wzbudzi twój niepokój, pojawi się dziwna wiadomość SMS, e-mail lub komunikat na ekranie komputera, koniecznie zadzwoń do banku, aby to zweryfikować.

14 Chroń swoje dane osobowe! Jest to najważniejsza zasada odnosząca się do bezpieczeństwa finansowego. Uważajmy na to, komu podajemy adres, telefon i numer dowodu osobistego. Często podajemy dane w dobrej wierze, warto jednak pamiętać o tym, że przestępcy posługują się takimi informacjami, aby na przykład założyć konto czy uzyskać kredyt online.

Bądź ostrożny, spokojny i czujny! Internetowy dostęp do konta, karty płatnicze i aplikacje mobilne to standard w bankowości. Korzystamy z rachunków, kupujemy i płacimy kartami w sklepach internetowych – zakres usług oferowanych przez banki wciąż się zmienia, a wraz z nimi pojawiają się nowe zagrożenia. Skimming i phishing jeszcze niedawno były egzotycznymi pojęciami, jednak teraz oszustwa tego typu są na porządku dziennym. Jednak jako klient banku nie stoisz na przegranej pozycji – wystarczy rozsądek i czujność. Powyższe wskazówki powinny pomóc zmienić złe nawyki. Korzystaj z usług bankowych ze spokojem i uwagą, a wówczas twoje pieniądze będą bezpieczne.

Fot. Happyalex, Pramith Srichaisuntikul, Leszek Glasner/123rf.com

RAPORT
bankowość elektroniczna

JAK WYKIWAĆ

POZNAJ TAJNIKI BEZPIECZNEJ BANKOWOŚCI ELEKTRONICZNEJ

Polska należy do światowej czołówki krajów z najbardziej rozwiniętą bankowością internetową. ***Uwielbiamy płatności telefonami, dostęp do bankowości elektronicznej i nowe technologie.*** *Wszystko dodatkowo ułatwiają nam banki, które również chętnie wprowadzają do swojej oferty coraz to nowe funkcje i udogodnienia*

Bankowość elektroniczna jest wygodna, prosta w obsłudze i bezpieczna – pod warunkiem że trzymamy się pewnych zasad. Przedstawiamy kilka zachowań, które pozwolą nam na zwiększenie bezpieczeństwa podczas korzystania z bankowości elektronicznej. Warto wyrobić w sobie te nawyki.

Bankowość elektroniczna to znak naszych czasów

Szybki dostęp do pieniędzy przydaje się w każdej sytuacji – w domu, w pracy, po pracy, w podróży. **Banki są świadome oczekiwań i potrzeb klientów – stąd bankowość elektroniczna, czyli internetowe systemy, które pozwalają na wygodne płacenie online.** To również historia zakupów, możliwość lokowania kapitału i oszczędzania. Bankowość internetowa jest niezwykle wygodna i dziś wielu z nas nie wyobraża sobie bez niej życia. Kto ma czas i chęci stać w długich kolejkach do okienka bankowego czy pocztowego, aby dokonać pojedynczej wpłaty, czy po to, by sprawdzić historię transakcji? To wszystko mamy dzięki bankowości internetowej. Wystarczy komputer, tablet lub telefon z dostępem do internetu. Bez dwóch zdań – bankowość elektroniczna to udogodnienie, z którego każdy z nas chętnie korzysta.

Poznaj swojego wroga

Wiemy już, że bankowość elektroniczna przydaje się nam w codziennym życiu. Chętnie z niej korzystamy, ale czy jest to w 100 procentach bezpieczne? Banki oferują nam skomplikowane zabezpieczenia i szyfrowanie, zapewniają nas o szczelności swoich systemów i bardzo często przypominają nam o zagrożeniach, które czyhają na nas na każdym kroku. Niestety, wielu z nas przewija i zamyka takie komunikaty bez czytania. To poważny błąd. **Większość kradzieży i ataków hakerskich nie byłaby możliwa, gdyby wszyscy byli świadomi zagrożeń.**
Pierwszy krok do bezpiecznej bankowości elektronicznej to poznanie swojego wroga. Haker nie nosi czarnych rękawiczek i kominiarki. Nie zaatakuje nas w ciemnej uliczce i nie przeszuka naszej torby w zatłoczonym autobusie. **Haker wykorzysta każdy nasz błąd i chwilę nieuwagi, aby wykraść nasze dane – loginy i hasła do bankowości elektronicznej, a następnie ogołoci nasze konta.** Jak się przed tym obronić? Wystarczy stosować się do kilku prostych zasad.

Postaw na silne hasła zabezpieczające

Wiele kont bankowych jest hakowana przez to, że użytkownicy nie poświęcili przynajmniej kilku minut na wymyślenie **silnego hasła**. Z miejsca odpadają takie propozycje jak „1234", „haslo" czy data urodzin.
Jak stworzyć silne hasło? Przede wszystkim powinno:

- być długie i składać się co najmniej z kilku nastu znaków;
- zawierać litery i liczby;
- zawierać małe i wielkie litery;
- zawierać znaki specjalne, takie jak $, % czy &.

Pamiętajmy o tym, że **czym dłuższe i bardziej skompilowane hasło, tym trudniej je złamać czy odgadnąć**.

Gdy haseł jest dużo, warto też skorzystać z menedżerów haseł, jak choćby **KeePass 2** – wtedy musimy stworzyć silne hasło do menedżera, a wewnątrz programu nasze hasła będą bezpiecznie przechowywane, a także w razie potrzeby można łatwo wygenerować nowe, bardzo silne hasła.

Zabezpiecz swoje urządzenia

Nowoczesna technologia pozwala nam na dostęp do internetu z dowolnego miejsca, w dowolnym momencie i z wielu urządzeń. Telefon, tablet i komputer służą nam każdego dnia do pracy i rozrywki. To urządzenia, z których możemy połączyć się również z naszą bankowością elektroniczną. Zadbajmy więc o to, aby połączenie było bezpieczne.
Jak to zrobić? **Urządzenia, z których obsługujemy nasze konto, powinny mieć zainstalowane legalne oprogramowanie, w tym programy antywirusowe i firewall** (zaporę broniącą komputer przed atakiem z zewnątrz). **Pamiętajmy też o aktualizacjach**, ponieważ luki systemowe są często wykorzystywane przez cyberprzestępców.

OSZUSTA?

Nie otwieraj wiadomości e-mail z podejrzanych źródeł

Wielu hakerów wykorzystuje naszą naiwność i ciekawość, wysyłając nam wiadomości e-mail z zainfekowanymi linkami lub załącznikami. **Wystarczy kliknąć na taki odnośnik lub otworzyć załącznik, aby zainfekować nasze urządzenie lub przeglądarkę internetową wirusem**, który prześle dane do logowania do bankowości elektronicznej hakerowi.

Jak rozpoznać podejrzaną wiadomość? Spójrzmy na adres domeny i sam adres e-mail. Jeśli będzie zawierał podejrzane znaki, powinno to wzbudzić twoją czujność. **Hakerzy są podstępni i często podszywają się pod różne firmy**, aby przekonać nas do otworzenia linku. Musimy stale mieć się na baczności. Wygrana najnowszego iPhone'a? Ktoś podarował nam niezłą sumkę? **Uważaj! To podstęp.**

Kontaktuj się z bankiem w razie potrzeby

Pamiętajmy o tym, że **bank nigdy nie prosi nas o podawanie haseł i loginów** poza stroną logowania do bankowości elektronicznej. Przedstawiciele banków kontaktują się z nami telefonicznie w celach marketingowych, aby przedstawić nam swoją ofertę. Nawet wtedy nie podawajmy danych dostępowych.

Wielu przestępców podszywa się pod banki i wyłudza hasła, więc trzeba mieć to na uwadze. Nie oznacza to jednak, że to my nie powinniśmy kontaktować się z bankami. Nawet powinniśmy. Jeśli jakieś nietypowe działanie na rachunku wzbudzi naszą uwagę, dostajemy dziwne powiadomienia przez e-mail czy SMS, **zawsze warto zapytać o to pracownika banku** niż popełnić błąd, który będzie nas kosztował całe oszczędności życia.

Uważaj na stronę logowania

Przestępcy często wykorzystują fałszywe strony logowania do bankowości internetowej. Ofiara myśli, że loguje się do swojego konta, a tak naprawdę zostawia login i hasło hakerowi. Takie strony często do złudzenia przypominają oryginalne witryny, jednak można je rozpoznać i tym samym uniknąć utraty pieniędzy.

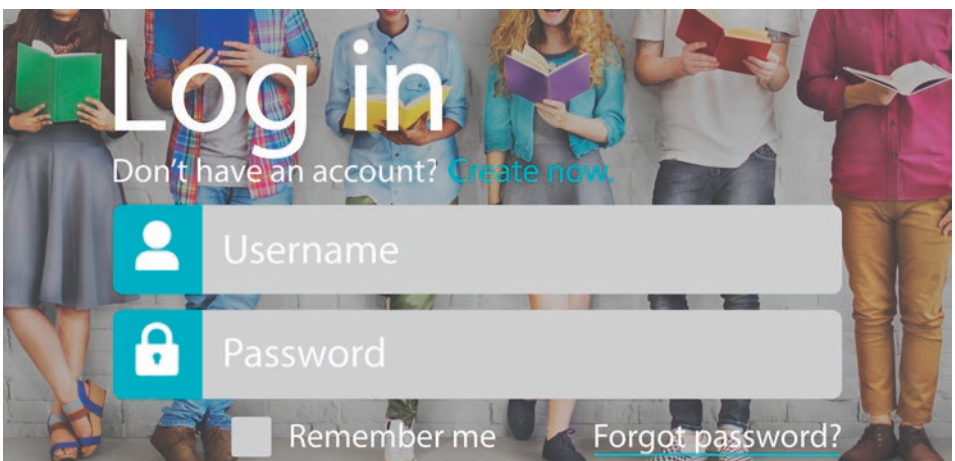
Jak rozpoznać fałszywą stronę logowania? Zwracajmy uwagę na **szyfrowanie połączenia i certyfikat bezpieczeństwa**. Pierwszy element można zidentyfikować po **symbolu kłódki** przy linku i skrócie **„https"** na początku adresu naszego dostawcy. Zielona lub zamknięta kłódka oznacza, że strona jest bezpieczna. Zwróćmy też uwagę na takie elementy, jak logo banku i dane oraz adres strony.

Postaw na kilkuetapowe logowanie

Hasło to niejedyne zabezpieczenie, który chroni nasze pieniądze. **Wielostopniowe logowanie staje się dziś coraz popularniejsze**, ponieważ nawet jeśli haker złamie nasze hasło, zawsze będzie musiał stawić czoło kolejnemu wyzwaniu – jeszcze trudniejszemu.

Podstawowa metoda dodatkowego zabezpieczenia to **kod SMS**, który musimy wpisać w podane pole po próbie zalogowania. Jeśli nie zrobimy tego w kilka chwil, zostaniemy ponownie poproszeni o login oraz hasło. To zabezpieczenie działa też jako podpis po każdym zleceniu płatności lub wypełnieniu umowy z bankiem przez internet.

SMS to nie jest jedyna metoda zabezpieczeń. Jest jeszcze **token**, który co jakiś czas generuje inny kod – musimy go wpisać w momencie logowania. Jest również elektroniczna wersja tokena, która działa jako aplikacja na smartfonie – **Google Authenticator**. Nie wszystkie banki stosują jednak te metody.



PILNUJ SWOICH LOGINÓW I HASEŁ

Każde konto bankowe i dostęp do bankowości elektronicznej chronione jest hasłem. Aby otrzymać dostęp do systemu, trzeba je podać wraz z unikalnym loginem, który jest przypisany przez bank. Pierwsza zasada bezpiecznej bankowości elektronicznej brzmi – **trzymaj swoje hasła i loginy w tajemnicy.** Podobnie jak numery PIN do kart bankomatowych, hasła i loginy muszą być strzeżone. Najlepiej, abyśmy nie zapisywali ich nigdzie i mieli je wszystkie w pamięci. **Pod żadnym pozorem nie zdradzajmy ich nikomu!** To najważniejsza zasada bezpieczeństwa.

Silne hasło możesz też stworzyć za pomocą aplikacji – generatora haseł. Taką wbudowaną funkcję ma najnowsza wersja przeglądarki Google Chrome. Możemy też skorzystać z innego rozwiązania, a w tym z:

- **https://generator.blulink.pl/**
- **https://www.dobrehaslo.pl/**
- **http://passwordsgenerator.net/pl/**
- **http://etechnologie.pl/generator-hasel/**
- **http://generator-hasel.webvisor.pl/**

Loguj się bezpiecznie i pamiętaj o wylogowaniu

Zawsze pilnuj urządzeń, z których logujesz się do bankowości elektronicznej, i nie zostawiaj ich bez nadzoru. Pamiętaj też o tym, żeby wylogować się z systemu za każdym razem. Nie trzeba być hakerem, aby wykorzystać otwarty rachunek bankowy.

Trzeba jednak trochę umiejętności programistycznych, aby zalogować się do sieci Wi-Fi i przez nią wykraść dane. Pamiętajmy więc o tym, aby łączyć się z internetem przez **zabezpieczone sieci, czyli takie, które posiadają hasło bezpieczeństwa i szyfrowanie**.

Hakerzy są sprytni jak zawsze, a my nierozważni jak nigdy – mamy zaufanie do płatności internetowych i systemów bankowych. Pamiętajmy jednak o tym, że nawet najbezpieczniejszy system nie ochroni naszych pieniędzy, kiedy podamy komuś hasła dostępowe. Przedstawione reguły działają jako solidna kłódka na drzwiach. Warto o nich pamiętać.

Fot. Sean Prior, Tuahlensa, Rawpixel/123rf.com

RAPORT
bankowość elektroniczna

SŁOWNIK BANKOWOŚCI ELEKTRONICZNEJ

*Poznajmy **najważniejsze hasła**, które przewijają się w artykułach na wcześniejszych stronach. Dzięki temu łatwo nam będzie zrozumieć, o czym mówią pracownicy banku i łatwo nam będzie odnaleźć się w świecie bankowości elektronicznej*

BANKOWOŚĆ INTERNETOWA

Umożliwia dostęp do konta przez stronę internetową banku. Wystarczy zalogować się na własne konto, aby móc wykonywać przelewy, złożyć wniosek o kredyt lub założyć lokatę. Nie ma konieczności instalowania dodatkowych programów.

BANKOWOŚĆ TELEFONICZNA I MOBILNA

Jak sama nazwa wskazuje, jest to rodzaj bankowości elektronicznej, który polega na zarządzaniu własnym kontem za pomocą urządzeń mobilnych – w tym smartfonów i tabletów. To nie tylko dostęp do rachunku bankowego przez telefon, ale również załatwianie wszelkich spraw związanych z obsługą klienta przez infolinię.
W ostatnim czasie bardzo popularne stały się aplikacje pobierane na smartfony, które umożliwiają zarządzanie kontem. Jest to świetny przykład bankowości mobilnej.

CERTYFIKAT UŻYTKOWNIKA

Jest to rodzaj poświadczenia tożsamości użytkownika podczas wykonywania operacji w systemie informatycznym. Banki w różny sposób generują takie certyfikaty. Jest to jeden z rodzajów silnego uwierzytelniania, który ma zapewnić najwyższe bezpieczeństwo.

CHARGEBACK

Rozwiązaniem zabezpieczającym interesy kupujących jest procedura chargeback, realizowana na zlecenie konsumenta przez bank. Jej celem jest zwrot środków na konto, do którego wystawiono kartę użytą do transakcji. Możemy zażądać przeprowadzenia tej procedury w razie oszustwa, pomyłki, ale także w sytuacji, gdy nie jesteśmy zadowoleni z jakości zakupionego towaru.

E-MAIL BANKING

Nasz e-mail służy nie tylko do odbierania nowych ofert kredytowych banku. Dzięki tak zwanemu e-mail bankingowi możliwe jest odbieranie dowodów wpłaty na skrzynkę pocztową w ciągu kilku sekund. Banki wykorzystują e-mail również do przesyłania wszelkich ostrzeżeń o próbie wyłudzenia danych oraz o trudnościach w dostępie do konta w przypadku prac konserwacyjnych.

KARTY BANKOWE

Karty wmożliwiają płacenie za usługi oraz produkty bez potrzeby posiadania przy sobie pieniędzy w fizycznej formie. Dodatkowo za ich pomocą możliwe jest wypłacanie banknotów z powszechnie dostępnych bankomatów. Karty debetowe i kredytowe wykorzystywane są również do wykonywania szybkich transakcji internetowych.

PODPIS ELEKTRONICZNY

To narzędzie umożliwiające identyfikację tożsamości klienta. Wymaga on posiadania odpowiednich urządzeń, które umożliwiają złożenie tego typu podpisu. Jest to jedna z najprostszych i najbardziej bezpiecznych form uwierzytelniania.

PROSTE UWIERZYTELNIANIE – IDENTYFIKATOR, HASŁO, PIN

Bardzo ważne w bankowości elektronicznej jest potwierdzanie autentyczności klienta. Niepowtarzalne hasło i unikatowy identyfikator, znane tylko klientowi oraz bankowi, znacznie zmniejszają ryzyko włamania się przez osoby niepożądane. O ile hasła i identyfikatory stosuje się głównie w bankowości internetowej, tak PIN wykorzystywany jest w bankowości mobilnej. To zazwyczaj 4-cyfrowy kod zabezpieczający, który znać powinniśmy tylko my.

PRZELEW Z POŚREDNIKIEM

Coraz częściej od konieczności ręcznego wypełniania formularzy i oczekiwania, aż środki dotrą do adresata, uwalniają nas systemy zautomatyzowanych płatności dokonywanych przez pośredników. Podczas wyboru formy płatności w internetowym sklepie klikamy na ikonę pośrednika (na przykład DotPay, PayU, Przelewy24 czy PayPal), po czym logujemy się do swojego banku. Tam już tylko zatwierdzamy gotowy przelew – kwota, numer konta odbiorcy, tytuł przelewu – wszystkie te dane są wpisane automatycznie.

SILNE UWIERZYTELNIANIE

Silne uwierzytelnianie to kolejny sposób na zwiększenie bezpieczeństwa bankowości elektronicznej, które dopełniają standardowe hasła. Popularnym sposobem takiego rozwiązania są zdrapki, kody SMS i tokeny.

SZYFROWANA TRANSMISJA DANYCH (SSL)

Przenosząc bankowość do internetu, konieczne stało się wprowadzenie odpowiednich środków bezpieczeństwa, które będą chronić klientów przed atakami hakerskimi i podszywaniem się przez oszustów. Dlatego powstał protokół SSL, który umożliwia zachowanie poufności przesyłanych danych. Jest on wykorzystywany przez wszystkie banki w Polsce. Jeśli w polu adresu strony internetowej widnieje zielony napis SSL lub symbol kłódki, masz pewność, że twoja transakcja jest zabezpieczona.

TOKEN

Token to inaczej generator kodów. Jest to niewielkie urządzenie, najczęściej wydawane klientowi osobiście przez bank, które po włożeniu karty oraz wpisaniu PIN-u będzie generowało kody, które następnie mogą zostać użyte do potwierdzenia przelewu. Ten popularny sposób jest jednym z rodzajów silnego uwierzytelniania, które ma służyć podnoszeniu bezpieczeństwa bankowości elektronicznej.

Komputer Świat od 1998 roku

Adres redakcji: 02-672 Warszawa, ul. Domaniewska 52
internet: www.komputerswiat.pl, forum.komputerswiat.pl
e-mail: redakcja@komputerswiat.pl
Daniel Kotliński: autor tekstów
Rafał Kamiński: redaktor naczelny
Tomasz Paczuski: z-ca redaktora naczelnego, szef wydania drukowanego
Agnieszka Al-Jawahiri: z-ca redaktora naczelnego, szef wydań specjalnych
Jolanta Rososińska: korekta
Robert Dobrzyński: dyrektor artystyczny
Mariusz Rybak: redaktor graficzny

ringier axel springer

Wydawca: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
Członek Izby Wydawców Prasy i Związku Kontroli Dystrybucji Prasy
www.ringieraxelspringer.pl, asp@axelspringer.pl
Adres: 02-672 Warszawa, ul. Domaniewska 52
tel. 22 2320000, 22 2320001

Prezes Zarządu: Mark Dekan
Prezes Honorowy: Wiesław Podkański
Dyrektor Generalny: Marcin Biegluk
Dyrektor Wydawniczy: Paweł Paczuski
Dyrektor Finansowy: Krzysztof Stopa
Dyrektor Sprzedaży: Mariusz Wąsiński
Dyrektor Marketingu: Olga Korolec

media impact

Biuro reklamy: Media Impact
reklama.warszawa@mediaimpact.pl
tel. (12) 2600200 (BOK)

Business Project Manager: Paweł Bulwan
Dział personalny: Monika Remiszewska
Księgowość: Katarzyna Fita (dyrektor)
Kolportaż: Rafał Kamiński (dyrektor)
Produkcja: Mariusz Gajda
Druk: Quad/Graphics Europe Sp. z o.o., Wyszków

Prenumerata i egzemplarze archiwalne:
tel. 22 3367901, infolinia 801000869;
e-mail: prenumerata.axel@qg.com (zamówienia)

Sprzedaż internetowa: www.literia.pl
Prenumerata zagraniczna: www.literia.pl
E-wydania: ksplus.pl

Redakcja nie zwraca materiałów niezamówionych, zastrzega sobie prawo redagowania nadesłanych tekstów, nie odpowiada za treść zamieszczanych reklam i ogłoszeń

Zabroniona jest bezumowna sprzedaż czasopisma po cenie niższej od ceny detalicznej ustalonej przez wydawcę. Sprzedaż numerów aktualnych i archiwalnych po innej cenie jest nielegalna i grozi odpowiedzialnością karną.